SANS SECURITY AWARENESS

BIPIMax

OUCH! | Desember 2017

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Amankan Akun Anda

Sekilas

Proses otentifikasi atau pembuktian identitas pengguna, merupakan hal utama dalam perlindungan informasi di dalam surel, media sosial dan akun bank daring. Mungkin tidak semua orang paham, ada tiga cara pembuktian siapa Anda; bisa dari apa yang Anda tahu – contohnya ialah sandi, apa yang Anda punya – contohnya adalah Surat Ijin Mengemudi (SIM) dan pribadi Anda – seperti sidik jari. Setiap metode memiliki keunggulan dan kekurangan. Salah satu cara otentifikasi paling sering digunakan adalah sandi. Namun, penggunaan sandi saja lama kelamaan tidak lagi ampuh. Edisi kali ini akan mengulas cara perlindungan diri dan pengamanan akun secara lebih baik dibanding penggunaan sandi saja. Cara ini disebut otentifikasi dua tahap.

Editor Tamu

Tiffany Schoenike adalah direktur kampanye dan inisiatif di National Cyber Security Alliance (**@staysafeonline**). Di tahun 2016, Ms. Schoenike bermitra dengan White House, pemerintah dan kalangan industri dalam pengembangan dan peluncuran program pengenalan Lock Down Your Login, a STOP. THINK. CONNECT.™ seputar otentifikasi dua tahap.

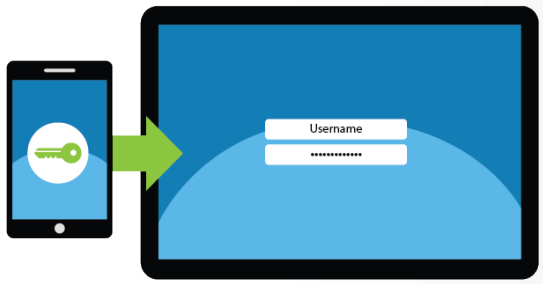
Sandi Tidak Lagi Ampuh

Sandi menguji keabsahan seseorang berdasar sesuatu yang diketahui Namun bila sandi tersebut berhasil ditebak atau diketahui pihak lain, mereka akan bisa mengakses akun Anda dan juga informasi yang ada. Bocornya sandi menjadi penyebab utama peretasan akun. Karena itu, disarankan menggunakan frasa-sandi yang lebih sulit ditebak, membedakan sandi setiap akun dan tidak berbagi sandi. Itu semua adalah saran yang baik tapi sandi lama kelamaan tidak lagi ampuh. Sekarang ada solusi sederhana dan cepat guna mengelola dan melindungi informasi pribadi, dikenal dengan sebutan otentifikasi dua tahap.

Amankan Akun Anda

Mengenal Otentifikasi Dua Tahap

Otentifikasi dua tahap (atau verifikasi dua tahap, otentifikasi multi faktor atau 2FA) lebih ampuh dibanding penggunaan sandi saja. Dalam penggunaannya, digunakan dua cara untuk menguji keabsahan penggunanya. Contoh terbaik adalah kartu ATM Anda. Saat menarik uang dari mesin ATM, sebenarnya Anda sudah menggunakan otentifikasi dua tahap. Untuk mengakses dana lewat ATM, diperlukan dua hal, pertama adalah kartu ATM itu sendiri (sesuatu yang Anda miliki) dan kedua adalah PIN (sesuatu yang Anda tahu). Bila kartu ATM itu hilang atau dicuri, tanpa PIN, orang lain tidak akan bisa menggunakannya. Si pencuri harus memiliki kartu ATM beserta PIN untuk bisa menarik dana. Otentifikasi dua tahap menggunakan konsep serupa.



Sebisa Mungkin Gunakan Otentifikasi Dua Tahap, salah satu langkah bijak dalam perlindungan daring Anda.

Cara Kerja

Otentifikasi dua tahap banyak digunakan di perbankan, surel, media sosial dan berbagai situs lainnya. Selain itu, biasanya akan diberikan tuntunan cara mengaktifkan otentifikasi dua tahap (simak daftar pustaka di halaman terakhir). Pengaktifan fasilitas otentifikasi dua tahap memicu urutan kerja berikut ini. Pertama, akses akun dengan menggunakan kode akun dan sandi seperti biasa. Ini adalah tahap pertama dari dua tahap – sesuatu yang Anda tahu. Selanjutnya Anda akan menerima kode tertentu yang dikirimkan ke gawas/alkom. Masukkan kode tersebut ke layar login. Ini adalah tahap kedua dari dua tahap, Anda harus menggunakan gawas/alkom untuk menerimanya. Setelah tahap itu, akun Anda benar-benar terlindungi dengan baik. Bila pihak lain berhasil mendapatkan sandi Anda, mereka tidak akan bisa mengakses akun Anda bila tidak memiliki gawas/alkom Anda.

Alih-alih menerima kode khusus via SMS, bisa juga menggunakan aplikasi otentifikasi khusus di gawas. Aplikasi ini akan memberikan kode tertentu setiap kali Anda hendak login. Penggunaan metode ini semakin meningkatkan keamanan karena

Amankan Akun Anda

kode khusus disiapkan oleh program aplikasi dan tidak dikirim lewat SMS. Lebih mudah juga karena tidak perlu terhubung dengan jaringan telpon. Progam aplikasi akan memunculkan kode baru pada saat Anda akan mengakses akun Anda.

Penggunana otentifikasi dua tahap tampak lebih merepotkan, namun informasi pribadi Anda bakal lebih terlindungi. Tidak perlu menunggu sampai akun Anda diretas, amankan akun dengan mengaktifkan otentifikasi dua tahap khususnya pada aplikasi surel, perbankan atau media sosial agar Anda semakin aman dan percaya diri.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi securingthehuman.sans.org/ouch/archives.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Daftar Pustaka

Frasa-Sandi:	https://securingthehuman.sans.org/ouch/2017#april2017
Situs Pendukung Otentifikasi Dua Faktor:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google Two-Step Verification:	http://www.google.com/landing/2step/

Dewan Redaksi: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Diterjemahkan oleh: T. Gunawan